Co-funded by
the European Union

EDDIE

EUROPEAN DISTRIBUTED
DATA INFRASTRUCTURE
FOR ENERGY

Identification and Authentication in a Common European Data Space

This work has been co-funded by the European Union's Horizon Innovation Actions under grant agreement No. 101069510

DOCUMENT INFORMATION

WP number and title	WP3 – Data Access Components
Deliverable number	
Version Number	V1.5
Document Reference	
Lead Beneficiary	FHO, ENT, D4G
Deliverable type	Report
Planned deliverable date	
Date of Issue	30/08/2024
Dissemination level	PU
Author(s)	Georg Hartner
Contributor(s)	Laurent Schmitt, Oliver Hödl, Shievam Kashyap, Stefan Grünberger
Keywords	

CONSORTIUM PARTNERS

The EDDIE Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Country
1	University of Applied Sciences Upper Austria – Campus Hagenberg – Research and Development	FHO	AT
2	Copenhagen School of Energy Infrastructure, Department of Economics, Copenhagen Business School	CBS	DK
3	European University Institute	EUI	IT
4	University of Vienna, Faculty of Computer Science, Cooperative Systems Research Group	VIE	AT
5	Austrian Institute of Technology, Center for Digital Safety & Security, Competence Unit Cooperative Digital Technologies	AIT	AT
6	The Lisbon Council for Economic Competitiveness and Social Renewal asbl	LIC	BE
7	PONTON GmbH	PON	DE
8	Asociación de Empresas de Energía Eléctrica (aelec)	AEL	ES
9	DEDA – Public Gas Distribution Networks – Single Member S.A.	DED	GR
10	EDA Energiewirtschaftlicher Datenaustausch GmbH	EDA	AT
11	Südtiroler Energieverband	SEV	IT
12	FlexiDAO	FLE	ES
13	Digital4Grids	D4G	FR
14	EASEE Gas	EAS	FR
15	Entarc.eu	ENT	AT
16	ETA+ GmbH	ETP	DE

DOCUMENT HISTORY

Version	Date	Status	Author(s), Reviewer	Description
V0.1	05/07/2024	Initiation	Georg Hartner	Create document, first version
V1.0	07/07/2024	Content addition	Georg Hartner	Major improvements, describe problem domains and eIDAS considerations
V1.1	08/07/2024	Content addition	Georg Hartner	Amend Domain-specific solution architectures
V1.2	10/07/2024	Revision	Oliver Hödl	Minor revisions
V1.3	23/07/2024	Review	Laurent Schmitt	Comments
V1.4	27/08/2024	Content addition	Georg Hartner	Add viewpoints of Third-Party CU Operators and Data Marketplaces
V1.5	29/08/2024	Review and Revision	Shievam Kashyap	Proof-reading, review and revisions
V1.6	30/08/2024	Revision	Stefan Grünberger	Revision, comments

AUTHOR AND REVIEWER ACKNOWLEDGMENTS

Author & Reviewer names	Partner
Georg Hartner	FHO, ENT
Laurent Schmitt	D4G
Oliver Hödl	FHO
Shievam Kashyap	FHO
Stefan Grünberger	FHO

DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Acronyms/ Abbreviations	Description
AS4	Applicability Statement 4 (a secure and reliable protocol for B2B communications)
CEEDS	Common European Energy Data Space
CIM	Common Information Model
CP	Connection Point
CU	Controllable Unit

DER	Distributed Energy Resource
DMD	Dedicated Measurement Device
DSO	Distribution System Operator
EDA	Energy Data Exchange Austria
EDDIE	European Distributed Data Infrastructure for Energy
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services
GAIA-X	A project aiming to develop common requirements for a European data infrastructure
I&A	Identification and Authentication
IAM	Identity and Access Management
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU	International Telecommunication Union
MQTT	Message Queuing Telemetry Transport (a lightweight messaging protocol)
MS	Member State
NC	Network Code
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
REST	Representational State Transfer (an architectural style for APIs)
SO	System Operator

VAT	Value Added Tax

EXECUTIVE SUMMARY

This document outlines the strategic considerations and architecture for implementing a streamlined, secure, and efficient Common European Identification and Authentication (I&A) system within the context of Project EDDIE and the broader European Data Strategy. It addresses four key challenges in data exchange within the Common European Energy Data Space (CEEDS): integration with existing federated data-sharing infrastructures, dynamic I&A for large numbers of distributed participants, platform orchestration, and data space connectors. The document proposes leveraging the electronic Identification and Authentication Services (eIDAS)[i] to maximize the use of common European I&A across these domains.

The paper details specific approaches for each challenge, including integrating with national onboarding processes, authenticating flexible customers and distributed energy resources, managing cloud-to-edge connectivity, and bridging EDDIE with other data spaces. It emphasizes the importance of creating a chain of trust between all involved parties and suggests using proven technologies like PKI infrastructure and digital certifications. The document concludes with key policy recommendations, such as mandating effortless eID/eIDAS authentication for both domestic and non-domestic eligible parties, considering edge control unit devices I&A with hardware type test certification, and defining reliable and commonly identified IDs for all connection agreement points and controllable units. These strategies aim to reduce market entry barriers, enhance security, and facilitate the development of a truly integrated European energy data space.

TABLE OF CONTENT

1 Purpose of the Document 10

2 I&A Challenges for Energy Data Exchange 11

3 Project EDDIE's Identification and Authentication Strategy 15

3.1 Domain D1 - Integration into (existing) regulated federated data-sharing infrastructures 15

3.2 Domain D2 - Highly dynamic I&A for large numbers of distributed participants 16

3.2.1 Identifying and authenticating a Flexible Customer 17

3.2.2 Identifying and authenticating a DER Unit 18

3.2.3 Identifying and authenticating a Controllable Unit Operator 18

3.3 Domain D3 - I&A for platform orchestrations 20

3.4 Domain D4 - Data Space Connectors 20

4 Key Policy Recommendations 22

5 References 24

LIST OF FIGURES

Figure 1 - Key I&A challenges for a streamlined CEEDS 11

Figure 2 - Linking standard cryptographic certificate infrastructure with Connection Point (CP) register 17

Figure 3 - Linking AIIDA I&A with eID. 19

Figure 4 - Data space bridge to link EDDIE with other data spaces 21

LIST OF TABLES

Table 1 - Recent regulatory push for a broader application of eID/eIDAS 14

1 Purpose of the Document

The purpose of this document is to explain the strategic considerations and architecture followed in project EDDIE to get to a streamlined, secured, efficient and common European way for Identification & Authentication (I&A). Project EDDIE – in line with the European Data Strategy sees a lot of potential in a broad adoption of electronic Identification and Authentication Services (EIDAS)[i] in its only recently amendment called the European Digital Identity Framework and proposes a target architecture to maximizing the use of common European Identification and Authentication to access the Common European Energy Data Space (CEEDS).

2 I&A Challenges for Energy Data Exchange

As described in Project EDDIE's broad vision (see Figure 1 below) on how to streamline data exchange in the energy sector, there are different challenges within the scope of a Common European Energy Data Space that require identification and authentication to be addressed in an appropriate manner, fit for the respective use case.

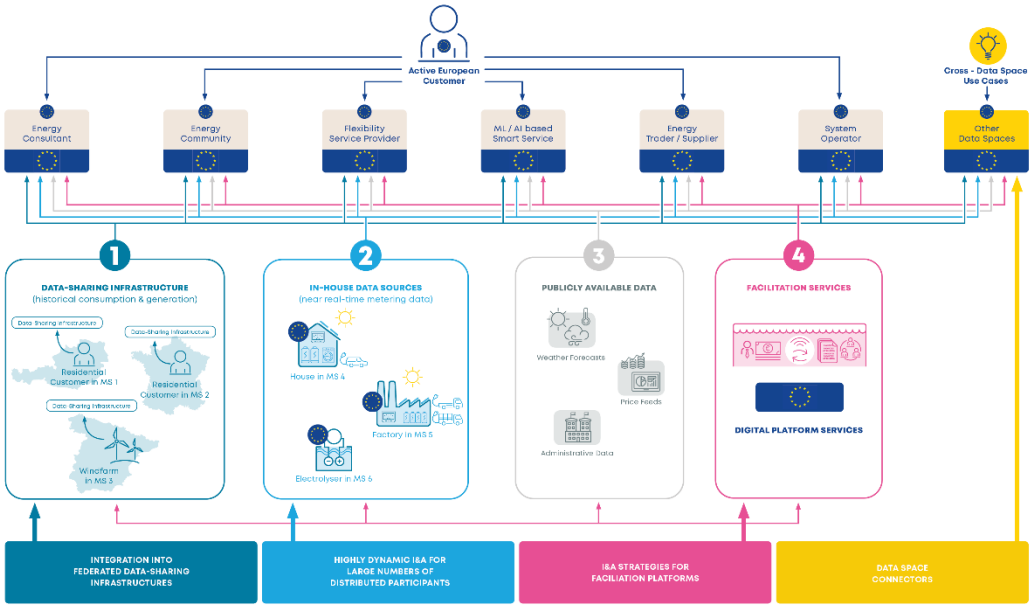

Figure 1 - Key I&A challenges for a streamlined CEEDS.

In this paper, we explain optimal solutions to respond to these 4 key challenges:

- **Domain D1 - Integration into (existing) federated data-sharing infrastructures.** As of Article 23 of Directive (EU) 2019/944[ii], the organisation of smart metering data management through regulated platform infrastructures different local bottom-up methods for identification and authentication. Hence, a CEEDS I&A strategy must integrate into such national requirements and rules. Also, the legal empowerment of the EC (Art. 24) clearly indicates that interoperability requirements shall be based upon existing national practices and so requiring such bottom-up options. Our EDDIE Framework has been designed to integrate with the different national onboarding and I&A mechanisms through a common consent facade pattern, allowing CEEDS users a uniform and easy-to-use consent management experience while remaining compliant with local national practices.

As laid out below, eIDAS and the Digital Identity Framework is expected to facilitate such consent facade harmonising as it allows to clearly distinguish roles across individual and private eligible party entities.

- **Domain D2 - Highly dynamic I&A for large numbers of distributed participants.** The crucial question of how to identifiably and securely manage a large number of participating end users and controllable entities, while protecting the data through edge components and secure communication and control structures, is more complex as it corresponds to a different deregulated, truly distributed infrastructure. eIDAS also offers an interesting option to manage data access at the cloud-edge level, and it incorporates proven-in-use encryption technology based on e.g. PKI infrastructures as core message as highlighted in the next chapter in this paper.
- **Domain D3 - I&A for platform orchestration.** To ease user access to our Eddie distributed data space infrastructures, the EDDIE framework provides 3 main facilitating components (*EDDIE Marketplace*, *EDDIE Admin Console* and *AIIDA Admin Console*) that are incorporating typical user, identification, authentication and authorization components like *KeyCloak* [iii] or standard web application security frameworks. The application of these technologies is considered standard best-practices and not specific to Data Space I&A considerations.
- **Domain D4 - Data Space Connectors.** EDDIE intends to exchange data with other data spaces, as a unified CIM based data dictionary to access critical sets of data across the whole energy value chain. As the EDDIE framework integrates both regulated and deregulated near real-time mission-critical processes, it streamlines its data access PI to maximise the use of public-subscribe real-time data exchanges that is complementary to the current published *Data Space Connectors* fit for the purpose of exchanging data at rest. Nevertheless, the EDDIE framework incorporates dedicated dataspace API – or better: the flexibility data space – to access other Data Spaces (for example OneNet [iv]). The following chapter explains the solution architecture for the cross-data space connectivity issue.

While the EDDIE consortium progresses through the implementation of its distributed data-sharing infrastructure across Europe, it is becoming obvious that current national markets

are not able to operate in a common single and European market today largely due to limitation in data exchange harmonisation as identified through the recent network code. Non-domestic market actors and solution providers are facing significant financial and legal hurdles before they can even gain access to consumer and market data from another member state. This represents a significant market entry barrier not just for the bare access to metering and consumption data, but also to participate in market communication e.g. for the provision of flexibility services as well as wholesale markets or the operation of platforms to facilitate Energy Communities. In fact, today energy related digital service providers must establish local operating companies in each respective member state, set up IDs via complex and formal structures just to be allowed to participate in market communication. This can easily represent data access costs of > 50.000-100.000 EUR per addressed MS – a big hurdle for start-ups and emerging solutions. The reason given is all too often that the operators of data-sharing infrastructure platforms need to reliably identify the acting parties. Moving forward, the European Strategy for Data has just identified a common and reliable way for identification and authentication as THE pillar for a common Digital Market. The tool to achieve this is *electronic Identification and Authentication Services (eIDAS)*[ii]. With eIDAS, natural persons can log in using their widely adopted SSA logins, sometimes also referred as *citizen IDs*, which are connected to their official identifications. National persons may represent and act on behalf of legal persons (companies or associations) or other national persons, if they are entitled to. eIDAS nodes from different member stated digitally *trust* each other, with the aim of accepting logins from different MSs. Project EDDIE's consortium partner Entarc.eu GmbH has already done a pilot implementation of the Austrian eIDAS node, and the team is driving things further to architect a streamlined integration of the technology into the Eddie I&A strategy.

Besides that, eIDAS also gains more and more traction into European legislation and regulation in the energy sector. The first push into applying the infrastructure in digital energy infrastructure was made in Commission Implementing Regulation (EU) 2023/1162[v], then still with a softer nudge, as the team was still waiting for an important revision of the eIDAS regulation. After its recent amendment as the European Digital Identity Framework, regulatory push could also be made more persuasive in the recent SO proposal for a new Network Code for Demand Response:

Commission Implementing Regulation (EU) 2023/1162	Common SO proposal for a new Network Code on Demand Response
Recital (12): Under this implementing Regulation, and to assist with the identification and the authentication of parties that are requesting access to data, Member States are recommended to encourage data access providers and permission administrators to support, as far as possible, digital solutions compliant with Regulation (EU) N°910/20146 ('eIDAS Regulation') to electronically identify and authenticate final customers and/or eligible parties. When doing so, data-access providers and consent administrators should make good use of already rolled-out national infrastructure. Using digital solutions should help increase the effectiveness of energy-related online services and transactions, and electronic business and commerce in the Union.	**Recital (n):** Using digital solutions should help to increase the effectiveness of energy-related online services and transactions, and electronic business and commerce in the Union. Currently, there are big hurdles for non-domestic parties. Current versions and amendments of eIDAS and national implementations support reliable cross-border authentication of natural and legal persons; in addition to that, also the representation of legal or natural persons by other natural persons. As many different platforms and diverse platforms are expected to play a role in the utilisation of balancing, congestion **management** and voltage control services, EU logins provide a solution to scattered credential management and means for service providers and CU Operators to offer their products and services on a common European market. **Article 40(4):** To ensure the secure and efficient identification and the authentication of parties, all flexibility register platforms shall – in addition to potential other means of authentication - support, as far as possible, digital solutions compliant with Regulation (EU) No ° 910/ 2014 of the European Parliament and of the Council (6) ('eIDAS Regulation') to electronically identify and authenticate service providers, CU Operators, systems operators and flexible customer. When doing so, flexibility platform operators shall duly consider already rolled-out national infrastructure.

Table 1 - Recent regulatory push for a broader application of eID/eIDAS.

3 Project EDDIE's Identification and Authentication Strategy

In the following paragraphs, we encapsulate how EDDIE is approaching the challenges of identification and authentication and how eIDAS as an EU solution may be integrated and facilitated.

3.1 Domain D1 - Integration into (existing) regulated federated data-sharing infrastructures

To properly interconnect with existing national process environments. The EDDIE Framework integrates *regional connectors* which require, the business entities using the EDDIE Framework to *onboard* themselves to corresponding national regulated environments. Associated processes for onboarding have so far been very diverse, and so the new Commission Implementing Regulation (EU) 2023/1162 requests member states to report the necessary alignment steps with a common reference model which the Eddie framework already anticipates (see *General Information* section in the reference model). The output and activities of current onboarding processes are very diverse across Europe – implicitly representing market entry barriers to foreign entities, some examples:

- In Austria business entities need to register at the industry association's website to get an identification and public/private key pairs to be used within the AS4-based communication with over 110 Austrian DSOs via *Energy Data Exchange Austria (EDA)*[vi],
- In France business entities get access to *Enedis Data Hub*[vii], through their registration at the data hub, using a French cell phone number for activation,
- In Spain, to be set up with *Datadis*[viii], business entities need to request a VAT for foreign companies to be used as their identifier,
- To use the API at Danish Energinet data hub, business entities need to establish a company to create an *MitID/BrugerID*[ix]. This represents a significant expense and hurdle that can also be observed in the Netherlands (with the requirement to receive an *eHerkenning*[x]) and some other MSs.

The Eddie dataspace framework has been designed to simplify identification of foreign business parties, starting with the elaboration of clear and comprehensive documentation to assist parties in that step. This **onboarding process currently represents one of the highest entry barriers for market parties wishing to scale across European markets**, while current national technical solutions can't spare eligible parties associated legal and administrative hurdles**.** The *EDDIE framework* provides opensource infrastructures that allows solution providers to reduce data integration costs and get going within weeks. We are convinced the application of eIDAS to reliably authenticate legal and natural persons would significantly reduce current pan European identification barriers of the EDDIE framework, aiming for common *onboarding using eID/EIDAS*, while keeping usual national practices, such as PKIs for AS4-based communication or OAuth solutions for the authentication with REST-based data hubs.

In addition to making onboarding more accessible, we are also recommending national data hubs to allow final customers and business actors to authenticate via European logins (eID/eIDAS) to follow the same chain of trust. This would avoid data exchange platform operators to manage separate credentials infrastructure and avoid media breaks.

3.2 Domain D2 - Highly dynamic I&A for large numbers of distributed participants

Authentication in this domain is managed through different vendor specific approaches while it represents a significant share of mission-critical private data for future flexibility data space. Connecting large numbers of small-scale flexible assets owned by residential private consumers inevitably places a challenge on how to identify assets and consumers and make them accountable for their actions and data protection. Of course, there are proven-in-use solution architectures to tackle that challenge at a generic level but integrating them together into real operational mission critical environment requires to adapt them to meet also the necessities and particularities of the energy sector. Also, in D2 it is important to close a chain of trust among all involved parties, where eIDs and eIDAS can contribute. In EDDIE, we have identified the following identification patterns:

- Identification and authenticating of flexible DERs (Heat Pumps, EV Charging, etc.) equipped with Control Units and Dedicated Measurement Devices enrolled by a Control Unit Operator and owned by a Flexible Consumer.

- **Identifying and authenticating a *Flexible Customer*** as the holder of the connection agreement to secure flexibility services and interactive use cases like e.g. *Flexible Connection Agreements*.
- **Identifying and authenticating a *Controllable Unit Operator.***
- **Identifying and authenticating users for the AIIDA Admin Console** and the mobile app coming with AIIDA (Administrative Interface for In-house Data Access).

The following paragraphs give an insight into the considerations to address these four matters.

PLEASE NOTE: The presented solutions are a preliminary proposal based on the current state of works. According to the plan, intensified work on this starts in Q3 2024. However, due to the necessity induced by regulatory activities we are proposing a first draft.

3.2.1 Identifying and authenticating a Flexible Customer

Here it is important to verify that the actor really exists and is entitled to act with the privileges of the holder of a connection agreement. Figure 2 shows a potential solution for the issue.

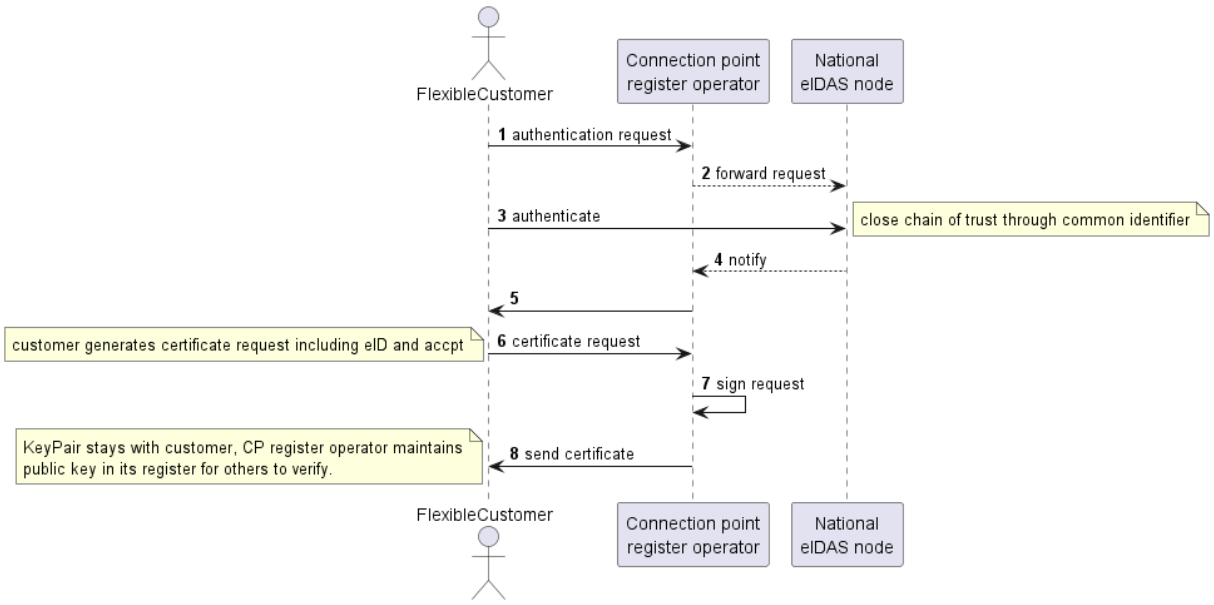

Figure 2 - Linking standard cryptographic certificate infrastructure with Connection Point (CP) register.

In this case, the *Flexible Customer* would send a typical certification request to the operator of the connection point register (typically the *DSO* in its role as *Connecting System Operator*, but there are also Member States featuring e.g. a *National Connection Point Register*). Whilst

the customer remains in full control as the only one holding both public and private keys, by signing the certificate with its private key, the Connection Point (CP) register operator confirms the entitlement of the eID to manage data related to the accounting point. Data exchange that is later signed with its private key can then be verified easily by checking it against the public key in the CP register. In turn, if the intended receiver is the Flexible Customer, data would be encrypted using the same public key, and the sender can rely upon the fact that only the Flexible Customer with its private key may de-crypt the message. This is commonly used practice and proven-in-use technology (since Nov 1988, latest update Oct 2021 - see ITU's *X.509* standard and *ISO/IEC 9594-8:2020*). It is also important that the transportation medium for that data to be used later may be whatever suits best for the use case (e.g. REST, AS4, Kafka, MQTT, DLTs, etc.), and that there is broad support in almost all related environments. Looking forward, issues related to quantum security are covered using stronger encryption strategies (e.g. *Elliptic Curve Certificates*). Developments on that end should be followed when setting up related infrastructures.

3.2.2 Identifying and authenticating a DER Unit

In this case, the DER unit would install local certificates through the DER control unit hardware confirming the flexibility products for which the DER has been type tested for. The associated Controllable Unit (CU) connection to CU Operators is encrypted according to that local certificate private key and the control unit operator public key while flexible consumers provide login credentials to certify their associated CU ownership as well as to authorise data exchanges with service providers available through the CU platform interface. Data exchanges between CU Operators and service providers are encrypted according to the authorised data exchanges digitally signed by consumers and CU Operators considering only flexibility products within the service provider portfolio for which the DER control unit has been type tested for.

3.2.3 Identifying and authenticating a Controllable Unit Operator

Controllable Units (CUs) as of the System Operator (SO) proposal for the Network Code on Demand Response form the smallest accountable unit for the aggregation of distributed flexibilities. They are aggregated by service providers (or also Energy Savings Applications or Energy Community Digital Platforms) and need to communicate with them. Service providers (and providers of other platforms) would – in the EDDIE scenario – use the EDDIE Framework to control and interact with a variety of on-premises or cloud-based CU Operators or directly

with Control Units using AIIDA interfaces, hence they need to manage associated trust and authentication schemas. It is also worthwhile to highlight that these relationships are highly dynamic and distributed, CUs/AIIDA instances will join and leave portfolios, and see other issues like failing connections – this needs to be reflected in an effective I&A strategy. Figure 3 shows a sequence diagram of the identification and authentication handshake designed to create a chain of trust and ensure further encrypted and signed communication between cloud and edge.

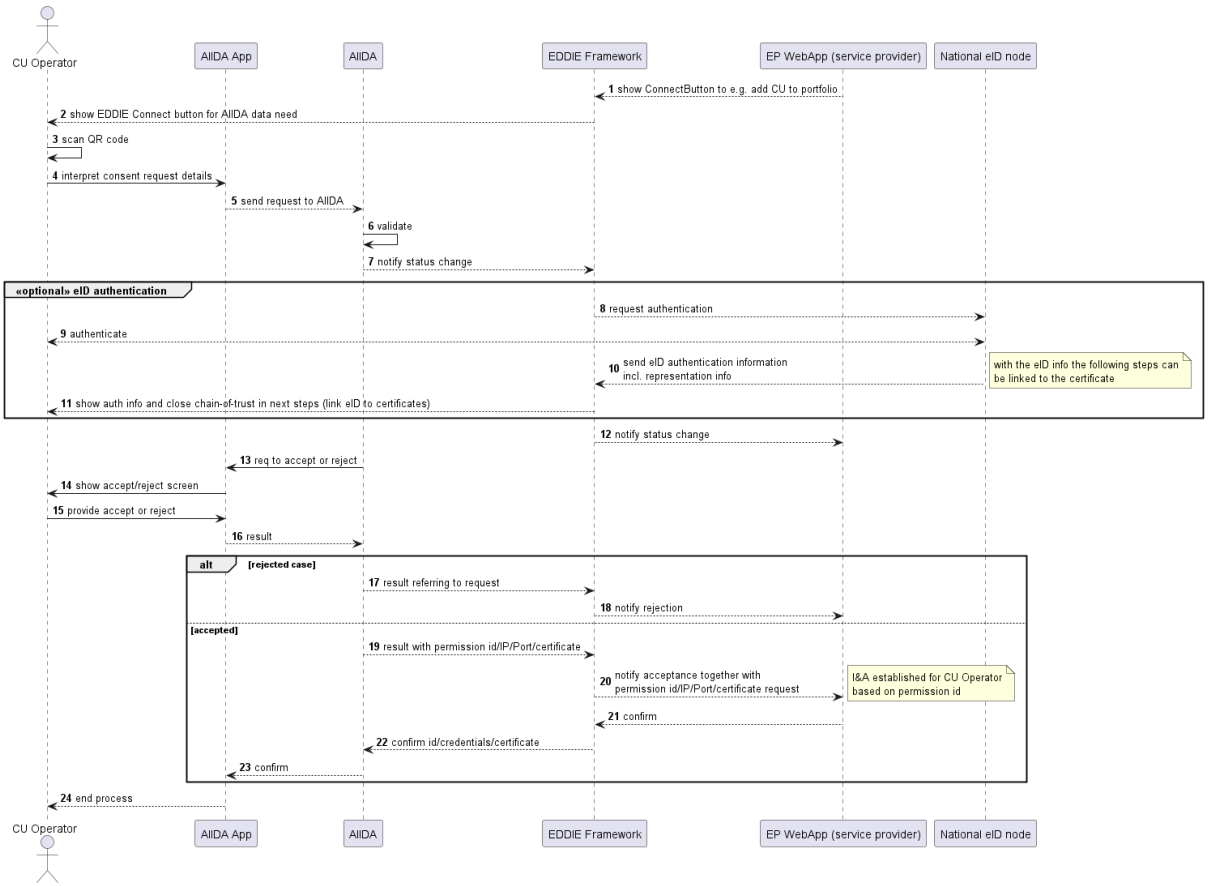

Figure 3 - Linking AIIDA I&A with eID.

Please note that the bottom case box (17-23) is considered absolutely mandatory and realisable with few external dependencies, as it is solely based on common PKI infrastructure. Steps 8-11 are optional and should be included to close the chain of trust between the eIDAS space and the authentication mechanisms tailored for secure cloud-to-edge interaction. For the latter, it will be examined until the end of 2024, if eIDAS-compatible tools and mechanisms are applicable to achieve also these requirements.

As agreed between Systems Operators and stakeholders in the SO proposal for new Rules on Demand Response, there will be *Cloud-Operated Controllable Units* a.k.a. *Third-Party CU*

Operators or *Technical Aggregators*. These service providers are operating CUs on behalf of the final customer through cloud infrastructure and take the responsibilities of a usual CU Operator. However, due to the simplicity of maintenance and deployment, this scenario is rather to be seen as very realistic and evenly justified in the future as on-premises deployments. Some MSs are already quite far in developing utility-led *Digital Customer Interfaces that can take that role on premises (e.g. AT/FR/NL/DE),* some are far away from that.

In any case, AIIDA supports both on-premises and in-cloud operation for a multiplicity of customers. Project EDDIE already operates first data services for Austrian Smart Meter Data both from on-premises installations and from OE-Smart Meter – Adapters connected to the cloud. The latter case allows for a multiplicity of sensors and *Dedicated Measurement Devices (DMDs)* to be connected to the Cloud-AIIDA Operator. IAM between DMD and AIIDA stays under control and responsibility of the OEM, the IAM between Cloud-AIIDA CU Operator and Data Space follows the standard patterns described above. In this case, also consent is managed through platforms and apps of the OEM rather than through the original AIIDA app.

3.3 Domain D3 - I&A for platform orchestrations

The orchestrated platforms connected with EDDIE use common web application security frameworks, such as *Keycloak* to manage users, roles and I&A. As many other web applications today, the Eddie framework is supporting eIDs as a means for authentication. This authentication is considered as a minimum base requirement but is not sufficient for facilitating the development of a Common European Energy Data Space which requires the development of authentication processes as described for D1 and D2.

3.4 Domain D4 - Data Space Connectors

To provide a seamless federation of EDDIE with other data spaces, and respecting EDDIE's role as a key enabler and major data source for other initiatives, EDDIE is providing *bridges* via the integration of Data Space Connectors for diverse technologies and environments. Figure 4 shows a schematic overview for such an integration that has been elaborated together with Austrian Institute of Technology (as GAIA-X[xi] Hub Lead for Austria).

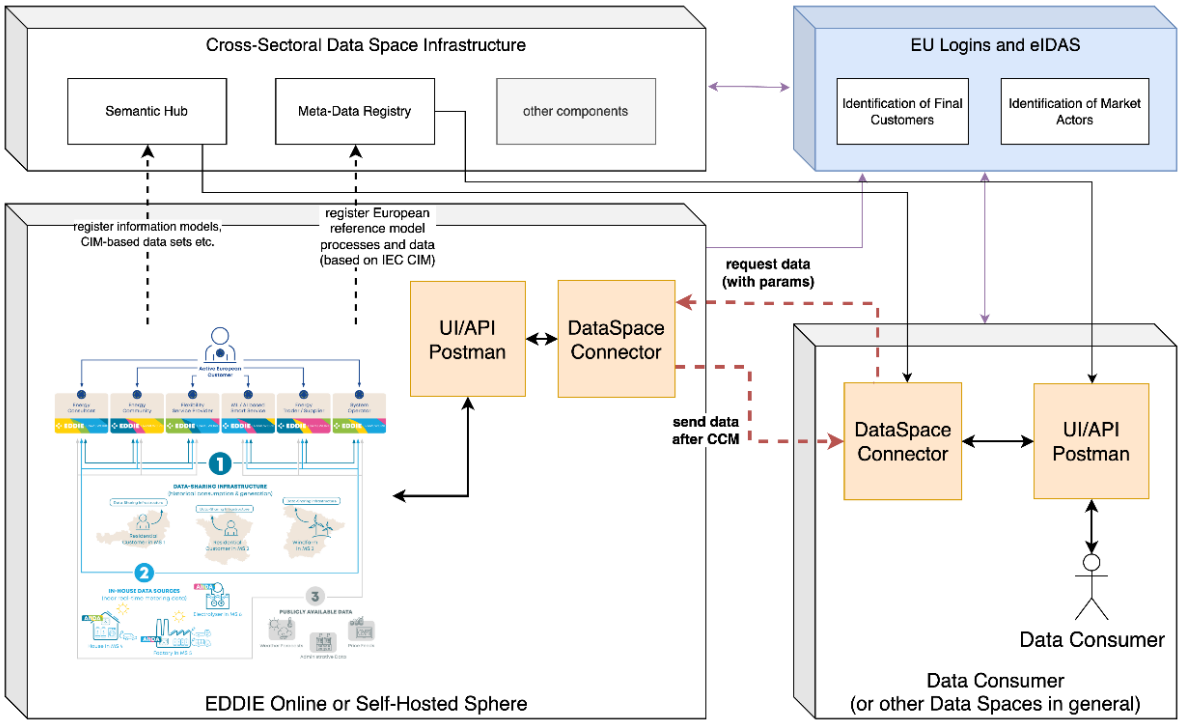

Figure 4 - Data space bridge to link EDDIE with other data spaces

These data space connectors will act as a bridge for consent (a.k.a. permission) – related processes and data access. Besides the fact that EDDIE is already linking national energy data spaces, the EDDIE Framework is focusing on establishing links with sister projects (e.g. *EnerShare*[xii], *Synergies*[xiii], *Data Cellar*[xiv], *OMEGA-X*[xv]) and *OneNet*. As an example, EDDIE will be registered as a *OneNet Service* that can provide connectivity with customer data, hence complementing the market-side data space.

4 Key Policy Recommendations

Number	Domain/ Priority	Explanation
1	D1/ Highest	**Mandate effortless eID/eIDAS authentication for domestic and non-domestic eligible parties onboarding alike.** This approach will allow existing digital platforms and market communication environments to keep their legacy credential management systems while opening up for European means of authentication. This is already very important for metering and consumption data access but will be much more relevant for all dedicated measurement device data access moving forward.
2	D1/ High	**Mandate national *permission administrators* and – if applicable - *metered data administrators* (as of CIR 2023/1162) to allow their (active and flexible) customers to authenticate via eID/eIDAS**, in addition to potentially existing legacy credentials management systems.
3	D2/ Highest	**When designing and defining the CEEDS, consider edge control unit devices I&A with their associated hardware type test certification.**
4	D2/ High	**Define reliable and commonly identified IDs for all *Connection Agreement Points, Controllable Units* and operators of *Controllable Units* (as of the SO proposal for the NC Demand Response) in all data exchange employed**. Linking cryptographic certificates with eIDAS and eID will create a common ground for identifying human and system actors while ensuring end to end data and system security.
5	D2/ Highest	**Reusing existing available technologies.** Already widely used PKI infrastructures and digital certifications cover necessary requirements.

6	D2/ High	**Define clearly the digital responsibilities of the connecting SO and Control Unit Operators in a CEEDS that includes cloud-edge connectivity.** Both operators can act as a *point of trust and reference* in highly distributed environments.
7	D3/ Medium	**Encourage deployment of eIDs/eIDAS on flexibility data exchange platforms in deregulated domains.** This will have a streamlining effect and efficiency gains in later developments, especially for distributed and diversified data environments where it is essential to have a commonly agreed trust anchor.
8	D4/ Medium	**Just as data management infrastructures for member states vary, it should also be accepted that different Data Spaces use different means for identification and authentication for their actual data exchange.** Different data exchange environments have been built for different purposes and have been architected with different goals in mind. However, put forward eID/eIDAS as a common ground and as a basis for common identities in a federated CEEDS.

5 References

[i] eIDAS Regulation and eIDs (https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation), last accessed August 29th 2024
[ii] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0944, last accessed July 8th 2024
[iii] Keycloak Open Source Identity and Access Management Framework, see https://www.keycloak.org/, last accessed July 8th 2024
[iv] OneNet Project – One Network for Europe, see https://www.onenet-project.eu/, last accessed July 8th 2024
[v] Commission Implementing Regulation (EU) 2023/1162 of 6 June 2023 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data, see https://eur-lex.europa.eu/eli/reg_impl/2023/1162/oj, last accessed July 8th 2024
[vi] Energy Data Exchange Austria (https://ebutilities.at) and EDA GmbH (https://eda.at), last accessed August 27th 20024
[vii] Enedis Data Hub, https://datahub-enedis.fr/, last accessed August 27th, 2024
[viii] DataDis platform, https://datadis.es, last accessed August 27th, 2024
[ix] BrugerID/MitID, https://www.mitid.dk/en-gb/ , last accessed August 27th 2024
[x] eHerkenning, https://www.eherkenning.nl/nl , last accessed August 27th 2024
[xi] GAIA-X, see https://gaia-x.eu/, last accessed July 8th 2024
[xii] EnerShare Project, see https://enershare.eu/, last accessed July 8th 2024
[xiii] Synergies Project, see https://synergies-project.eu/, last accessed July 8th 2024
[xiv] Data Cellar Project, see https://datacellarproject.eu/, last accessed July 8th 2024
[xv] OMEGA-X Data Space Project, see https://omega-x.eu/, last accessed July 8th 2024